A genealogy of hacking

Article (Accepted Version)

Title: A Genealogy of Hacking

Professor Tim Jordan, University of Sussex

Word Count: 8,253 (9,554 with Bibliography included)

Abstract: Hacking is now a widely discussed and known phenomenon, but remains difficult to define and empirically identify because it has come to refer to many different, sometimes incompatible, material practices. This paper proposes genealogy as a framework for understanding hacking by briefly revisiting Foucault's concept of genealogy and interpreting its perspectival stance through the feminist materialist concept of the situated observer. Using genealogy as a theoretical frame a history of hacking will be proposed in four phases. The first phase is the 'pre-history' of hacking in which four core practices were developed. The second phase is the 'golden age of cracking' in which hacking becomes a self-conscious identity and community and is for many identified with breaking into computers, even while non-cracking practices such as free software mature. The third phase sees hacking divide into a number of new practices even while old practices continue, including the rise of serious cybercrime, hacktivism, the division of Open Source and Free Software and hacking as an ethic of business and work. The final phase sees broad consciousness of state-sponsored hacking, the re-rise of hardware hacking in maker labs and hack spaces and the diffusion of hacking into a broad 'clever' practice. In conclusion it will be argued that hacking consists across all the practices surveyed of an interrogation of the rationality of information techno-cultures enacted by each hacker practice situating itself within a particular techno-culture and then using that techno-culture to change itself, both in changing potential actions that can be taken and changing the nature of the techno-culture itself.

Keywords: hacking, hacktivism, cybercrime, open source, free software

A Genealogy of Hacking

Introduction

Despite twenty years of ongoing research into hacking, it remains unclear what hacking means. For example, in the 2010s the idea of the hack was complicated by the UK 'phone hacking' scandal, a set of practices mostly quite distinct from breaking into computers. (Davies, 2014) While some accounts now locate a 'narrow' or 'pure' sense of hacking in illicit remote breaking into computer systems, there are also abstract and general accounts such as those of Himanen and Wark that describe a particular social practice as hacking and open up the possibility of hacking virtually anything, as can be seen in such things as ‘lifehacking’. (Wark, 2004; Himanen, 2001) As the importance and widespread awareness of hacking has grown, its meaning has remained difficult to grasp. Further, hacking as a computer mediated practice has now been around for some time and has undergone change, we have memories of hacking.

I will argue that hacking should be understood as practices that express the rationality of information techno-cultures. I will do this by suggesting that a return to Foucault's concept of genealogy and extending that concept through feminist materialism creates a frame for analysis that clarifies hacking's meaning. A history of hacking formed within this genealogical frame is then outlined in four phases: multiplicity in the pre-history of hacking; the golden age of (cr)hacking; hacking divisions; and, hacking as both triumphant and lost. This paper then concludes by arguing on the basis of this four part history that the nature of hacking and its place in twenty-first century society is that hacking expresses the rationality, in the sense of logics and discourses, of information techno-cultures. Hacking reveals the logics of the inter-section of information technology and

information cultures in their constant information technology-enabled actions that recreate the same technologies to enable different actions.

Genealogy and a Genealogy of Hacking

Foucault argued in the early 1970s for genealogy as an approach to understanding the past into the present. (Miller, 1994; Macey, 1994) Without surveying the extensive and significant literature on this topic, I will reiterate the essential ideas of genealogy and develop them briefly though a key feminist intervention to create a framework for analysing hacking. Accordingly, this framing is not meant to be a comprehensive treatment of such a genealogical frame but it provides a way of refining the nature of hacking.

Three different ideas underpin Foucauldian genealogy and these can then be exemplified through the tactic of refusing an origin as explanation. The first idea is that genealogy is anti-teleological and does not read history from the point of view of either the 'now', seeing past events as significant only if they lead to our present state, or in a closely related way, the 'victor', seeing past events as significant only if they contributed to whoever holds power in the present. Second, genealogy looks to those things that might seem to be without history—love, sexuality—and pays attention to their functioning in action. Last, genealogy pays attention to phenomena being absent and seeks whatever significance absences might suggest. These three ideas come together in the rejection of origins as a valid explanatory principle.

> From the vantage point of an absolute distance, free from the restraints of positive knowledge, the origin makes possible a field of knowledge whose function is to recover it, but always in a false recognition due to the excesses of its own speech. The origin lies at a

> place of inevitable loss, the point where the truth of things corresponded to a truthful discourse, the site of a fleeting articulation that discourse has obscured and finally lost.
>
> (Foucault, 1977, p. 143)

An example of origin as explanation will be familiar to those who have done almost any reading or research on hacking in the role Steven Levy's articulation of the 'hacker ethic' has played in understanding hacking. (Levy, 1984) Levy's is an influential work of journalism creating an origin for hacking by writing a history of hacking whose spirit he summarised in six principles. These principles then function as an origin story for hacking articulated in the sense that they reappear often as the definition of hacking that coalesced at its origin. In short, after Levy the idea of the hack as an unexpected and brilliant piece of technological detournement as defined in Levy's ethic became the self-referring origin of and explanation for hacking. To construct a genealogy of hacking we must be suspicious of this origin story, so often repeated, where the ethic of hacking emerges in the model train club of MIT, their allies and cognates and their penchant for technological tricks. We only need to refer to the (so far) unwritten histories of Fidonet (a worldwide network of home computers connected via phone lines), the European computer groups Chaos Computer Club or XS4ALL to suggest differences to Levy’s largely USA-based story.

The use of genealogy for understanding hacking is suggested by the suspicion toward Levy and origins. Foucault's argument is that pursuit of the origin is always disappointed by historical analysis which does not find 'a timeless and eternal secret' but the mess of interactions. He gives the example that the pursuit of the origin of reason shows it to have been born in chance in the passionate arguments of scholars or that the origin of liberty can be seen to be an invention of the ruling class and not an inviolable element of human nature. (Foucault, 1977, p. 142) Instead of the unity and truth offered by the origin Foucault argues, 'What is found at the historical beginning of

things is not the inviolable identity of their origin; it is the dissension of other things. It is disparity.' (Foucault, 1977, p. 142) This leads to a further point about genealogy because finding difference in the origin does not destroy history but instead supports the recognition that histories can be told but must each be partial and address their partiality through evidence—here is the reason Foucault calls genealogy 'grey, meticulous and patiently documentary' (Foucault, 1977, p. 139). Even if there is no 'truth in origin' to be uncovered then there remains the construction of evidence-based, partial histories (like the one I will offer below).

> The affirmation of knowledge as perspective. Historians take unusual pains to erase the elements in their work which reveal their grounding in a particular time and place, their preferences in a controversy—the unavoidable obstacles of their passion. Nietzsche's version of historical sense is explicit in its perspective and acknowledge its system of injustice.
>
> (Foucault, 1977. P. 156-6)

The consequence of difference at the origin is that history's objectivity must be built on partiality in evidence. This is not as startling a claim now as it perhaps was when Foucault made it, but the reasoning behind it is worth repeating because if we can take at face-value the idea of patient documentation as an understanding of evidence, it remains somewhat unclear what partiality means here. To understand this a useful addition to Foucault is the feminist[1] argument about the importance of the situated observer. (Letherby, 2003; Harding and Hintikka, 2003)

> Above all, rational knowledge does not pretend to disengagement: to be from everywhere and so nowhere, to be free from interpretation, from being represented, to be fully self-contained or fully formalizable. Rational knowledge is a process of ongoing critical

> interpretation among 'fields' of interpreters and decoders.
>
> (Haraway, 1991, p. 196)

Here Haraway argues for a rejection of the 'gods eye' view that sees everything from nowhere. If knowledge is never about everything and from nowhere then it has to be situated; knowledge has to come from somewhere and be based on something. Objectivity can therefore never be the authorisation by nature or an external ontological reality of claims but must instead be generated knowing that the objectivity comes from the nature of the evidence and arguments marshalled for a claim. Barad's complex argument is a persuasive articulation of this point "“objectivity” is not preexistence (in the ontological sense) or the preexistent made manifest to the cognitive mind (in the epistemological sense). Objectivity is a matter of accountability for what materializes, for what comes to be.' (Barad, 2007, p. 361)

Geenealogy is best understood as exploration through a situated observer, who through the nature of their work, their evidence and their arguments, puts forward materialist conceptualisations and materialist claims about the world. Any such claims need to be made but also need to be made in relation to other claims and to be clear in their own situatedness. If there is any way of summarising this then surely Haraway puts it best as '*pleasure* in the confusion of boundaries and *responsibility* in their construction.' (Haraway, 1991, p. 150).

Genealogy in the sense I have proposed here is a frame for creating particular projects. For example, within the broad definition of genealogy, Foucault described his own genealogical project as being three part:

> First, a historical ontology of ourselves in relation to truth through which we constitute

> ourselves as subjects of knowledge; second, a historical ontology of ourselves in relation to a field of power through which we constitute ourselves as subjects acting on others; third, a historical ontology in relation to ethics through which we constitute ourselves as moral agents.
>
> (Foucault, 1997, p. 262)

I propose, in this spirit, a genealogy of hacking may be understood as part of a historical ontology of information technology through which we constitute ourselves as digital subjects in which hacking expresses the rationality of information techno-cultures. Rationality here does not refer to an abstract ahistorical logic, but to the situated repeated logics that also involve recurrent expressions that make up hacking's community of practice. It is tempting to call the repeated expressions that logics require to run, such as the judgements on good or bad practices, a 'poetics' of information techno-cultures but this would stretch what must be a limited conceptualisation. As Haraway argues, this is rationality as a 'process of ongoing critical interpretation' among actions and their interpreting actors in a field. In this sense, the frame of rationality as repeated logics, that are understood to involve recurrent cultures, interpetations and expressions, allows me to situate myself as a researcher on hacking in relation to hacking and to move to explain what the rationality of information techno-cultures might be by examining hacking practices; that is, the way hacking creates certain digital subjects.

A History of Hacking: A Partial Presentation

A genealogical project is constituted by histories that have an acknowledged and evidential partiality. The evidence about hacking my viewpoint can marshal argues for four broad stages in hacking over the last twenty or more years: a period of multiple cultures colliding with

computerisation and network technologies; a crackers' 'golden age' where breaking into a computer became identified with hacking; a re-division in which new kinds of hacking and the resurgence of Free Software hacking expanded and differentiated hacking while exposing core practices; and, a de-differentiation in which the meaning of hacking began to dissipate into such varied and multiple uses that its distinctiveness is sometimes hard to see. The evidence I have accumulated rests within the partiality of my organisation of this evidence but also derives from a wide range of accounts from the more informal and less academically 'legitimate' end of the long discussion with hackers and hacker analysts, through to interviews, log files, checking and cross-referencing evidence others have collected and integrating all this into projects of my own. My partiality frames my account but it does not undermine the evidence about the empirical mess of the universe of hackers in their everyday practices.

The phases I identify are broadly sequential, though with unclear boundaries, but they do not destroy each other, rather they accumulate practices of technological differentiation that articulate strongly or weakly against each other at different times and they include points at which new or previously obscure practices may suddenly become dominant and inescapable. For example, Free Software hacking endures through all phases while contributing some of the core cultural and technological practices of hacking but Free Software's practices were also eclipsed and seemed to exist underground in the 'golden age' only to resurface such that 'Free''s corruption into 'Open' has become applicable to many social practices. To explicate the claim that such a genealogical account can demonstrate that hacking is the rationality of information technology it is important to outline these phases and their characteristic practices. It is in these practices that a consistency of mediation and re-mediation of technologically determining contexts can be found that explicates a rationality characteristic of information techno-cultures.

Phones, Trains and Mainframes: A History of Hacking Part 1

The beginnings of hacking are perceivable in four threads that inter-sected and flowed around each other, not forming an originary assemblage but connecting differentiations in complex ways. (Jordan, 1999b; Taylor, 1999; Thomas, 2003) The early and multiple threads of hacking as the internet emerged into wider use were: conceptions of cyberspace as a place; techniques for manipulating materialised information; communities in virtual environments; and, the rise of programming as a profession involving both free software programmers and the programming proletariat. These will be outlined in turn.

Early in the emergence of the mass use of networked computer communication, including non-internet networks such as local bulletin board systems or globalised computer mediated communication such as Fidonet (a globally connected network of home computers), the idea grew that wherever discussions were occurring could somehow be conceptualised spatially. There was a sense that there was a 'place' out there in between all the non-virtual seats people were communicating from. Whether in the early illicit conference calls phone phreaks (a term for those who manipulated phone networks) set up or in voluminous posts in places like major discussion forum Usenet, many expressed a sense that they were going 'somewhere' even though they were sitting at a computer typing. This further led to the sense that this place and space, often called cyberspace, had its own ethics and politics; broadly understood cyberspace had its own values. Optimists argued for an ethics based purely on the merit of the words people were contributing, pessimists pointed to the persistent rudeness and abuse (or flaming); and both were probably right. Hacking emerges within this sense that cyberspace is a place with its own values. (Brooks and Boal eds, 1995; Jordan, 1999a, pp. 37-9; Barlow 1996; Brunton, 2013)

Techniques for altering technologies that were centred on manipulating information also emerged. These came from several sources, perhaps most powerfully from phone ‘phreaks’ who manipulated telephone communication and who were themselves often inspired by ham radio but also (famously in Levy's account) by running a complex model railroad, pranks and lock picking. These are manipulations of technologies to do things technologies were not designed or expected to do. While such clever uses of technology are not restricted to hacking, hacking gains part of its character from such grassroots and 'do-it-yourself' attitudes to manipulating information technologies. In particular, a dynamic emerges within contexts defined by information networks by which it is often difficult to prove someone has successfully manipulated a technology unless the manipulation is taught to someone else. If someone successfully unpicks a lock, you can see the lock opened, but manipulation over a network is often hard to prove unless someone is also shown how to undertake the manipulation. This is not true of all manipulations, software for example can simply be run to prove it works, though proving some coding was an elegant or clever solution probably involves showing how it was written, in effect undertaking training in the solution. In a significant number of networked information contexts the manipulation of technologies can only be proven if others are also shown how to manipulate the technology. This means that not only are there a range of techniques for changing information technologies but that this also produces a dynamic of peer education in making such changes. (Lapsley, 2014; Jordan, 2008; Levy, 1984; Taylor, 1999)

Related to, but also distinct from, both the conception of cyberspace as a place and the generation of information manipulation techniques applied to that place is the emergence of a sense of community in online places. Rheingold famously called these virtual communities and these have in the twenty-first century grown to mass use particularly through various implementations in social media networks. Often initially text based these places developed social relations such that particular collectives or communities came into being. While community is a complex and difficult to define

concept, here it generally refers to an online space in which the everyday is enacted. This also gives rise to the sense of sub-communities and sub-cultures that find a place on the internet because it can overcome isolation and distance, enabling those who might have particular interests to find others like themselves. Many 'virtual communities of interest' emerged, among them hackers who developed such things as journals and face to face conferences, through which their common interests underpinned an emerging community. (Rheingold, 1994; Kollock and Smith, 1998; Goldstein, 2008)

Last of these four inter-weaving threads is the emergence first of computer programming as a distinct and recognised skill and then its formation into a profession and potential source of employment. Early programming was so closely associated with specific machines that it only became recognised as a distinct skill as computers proliferated and began to grow in use. Two consequences structured the emergence of the profession of programming for hacking. First, the profession bifurcated between free software and the programming proletariat. The activity of coding is the same for both and individuals may, and often do, occupy both positions but there are distinct roles as a coder for community owned and collectively generated programmes and coding for governments and corporations for national interests or for profit. This is a broad distinction but it develops and begins to underpin many of the political aspects of coding. The second consequence was the realisation that coding determines and can re-determine the infrastructure of networked environments and that coding is itself based primarily on expertise in coding, with the hardware needed to code often far less than that needed for using complex programmes or for some other online activities like gaming. Expertise that can be won by reading manuals, being tutored by others online or through training then became a path to altering and evading the infrastructures of the internet and networked environments. (Rosenberg, 2008; Williams, 2012; Jordan, 2008)

Cutting across all these threads and setting up a consistent and persistent set of unequal social relations in hacking is the way early on and then in different ways, hacking has been gendered as patriarchal. Not only does hacking exist in the context of the rise of computer science, with its persistent masculine bias in both numbers and behaviours, but as the movement at the transgressive end of computing hacking has sometimes exaggerated the misogyny in computing. (Corneliussen, 2012; Jordan and Taylor, 1998, pp.767-8) Whether in online harassment or in practices which exclude women and conceive them as unable to hack, hacking emerged as a community with a strong thread of masculinity and practices that exclude female programmers. Though variable in time and place, this began and will remain an ongoing characteristic of hacking that is also embedded in wider issues of online abuse. (Shepherd et.al. 2015)

Together these threads inter-weave and contribute to the early emergence of a sense of hacking in computer networked environments. This might seem obvious from our present standpoint but at the time these kinds of developments were uncertain and things like John Perry Barlow's 'A Declaration of the Independence of Cyberspace' or hacker The Mentor's 'The Conscience of a Hacker' came as moments of clarity that articulated some of these threads and their meaning. Often these were moments of self-realisation, where a community came to recognise itself as such and not just as small isolated groups. This is not a unique process, for example there is Peterson's account of the emergence of roleplaying gaming that tells a similar story, but for hacking this process included these four threads. (Peterson, 2012) In this recognition, and even this early in such an inchoate set of material practices and thoughts, an interweaving emerges across practices of reforming technologies while also using them, which means relying on the technologies that are being changed. This interweaving even now can be seen as a way of both uncovering and forming the logics of information techno-cultures.

The Golden Age of (Cr)Hacking: A History of Hacking Part II

The 'golden age' of hacking refers to a time when the distinction of cracking and hacking all but disappeared (and it should be noted was hardly a golden age for computer administrators or security professionals). (Sterling, 1992; Thomas, 2005) 'Cracking' usually refers to illicitly breaking into someone else's computer through a range of techniques, such as social engineering (tricking someone into giving access) or exploitations of technical faults. A focus on cracking in police arrests and media publicity, along with a widening interest in 'exploring' computer and network technologies, led during this period to a near identification of cracking and hacking, something often contested only within (at the time) arcane and obscured communities such as the still emerging free software programming community or the cypherpunks. (Levy, 2001) Three different frames can be used to understand how the threads discussed in the previous section were integrated, fragmented and reformed in this period as hacking developed as a self-conscious and widely noticed community of practice; hacking as an intellectual pursuit; hacking as a political community; and, the almost unnoticed growth of other kinds of hackers. Again across all three we can trace the way they engage with technologies that create certain limited fields of action in order to then alter those technologies and recreate new limited fields of action.

The sense of cyberspace as a place with both communities and a particular politics or set of values in which certain techniques were used to alter information infrastructures were ideas already developed by the 1990s (as noted earlier). These ideas now came together into the view of hacking as breaking into networked systems primarily for intellectual exploration. This is one of the meanings of hacking that can be hard to recall as the twenty-first century unfolds, for reasons that will become clearer in the subsequent phases of hacking when cracking develops large-scale criminal and nation-state sabotage and surveillance practices. Yet a consistent thread through

hacker stories, interviews and retellings of their exploits in the period is that they cracked open sites by technical innovation, by tricking operators, by finding faults in software and other means and having cracked open sites explored them primarily for the intellectual thrill of being able to work out the problems that needed to be solved to break in. Whatever the technique used, the practice is one of taking certain disallowed actions (accessing the computer) and altering the technologies to create new actions (access). Hackers in this time established practices that are evidence of this focus on intellectual exploration. For example, hackers became known for breaking into systems and then telling the controllers of those systems how they had done it and giving (usually unwanted) advice on how to fix things. Hackers took up various common practices of academics and others who wish to share information, public conferences and journals being two obvious ones and neither of which are generally the practice of criminal sub-cultures. (Taylor, 1999; Jordan and Taylor, 1998; Mitnick, 2012; Littman, 1997, 1996; Quittner and Slatalla, 1995; Hafner and Markoff, 1991)

Emphasising intellectual exploration as a key component of the 'golden age' does not mean that hacking as cracking was ‘innocent’. There were the costs of fixing systems that were broken into or simply of tracking down those who had broken in. Damage was sometimes caused when a hacker's expertise was not as great as they thought. There were times these techniques led to criminal actions, such as rigging phone systems to win cars in radio phone-ins (Littman, 1997), and, perhaps more commonly, sometimes crime was needed to continue hacking (for example, in paying phone bills or replacing computer equipment). (Hafner and Markoff, 1991; Littman 1996) But this kind of crime was largely overshadowed by breaking into other people's virtual places for the sake of solving the problem of how to break in. Cybercrime then, in this period, was a confused category usually referring to those not seeking to gain except for intellectual adventure but whose illicit electronic break-ins were increasingly criminalised no matter what the consequence or motivation of the break-in. To hackers, perhaps somewhat blind to the problems their 'adventures' caused others, the

criminalisation of their explorations was akin to criminalising solving math problems. (Wall, 2008; Jordan and Taylor, 1998, pp. 773-5)

Hacking as a recognised and self-conscious community formed during this period, with small groups appearing and networking mechanisms like online bulletin board systems, conferences and journals growing. At the same time, some controversies that received widespread media attention not only ensured hacking was widely understood as cracking but that hackers also found themselves being presented back to themselves as crackers. Controversies like Kevin Mitnick's pursuit and arrest, which involved Mitnick being jailed and appearing on the front page of the New York Time as the first 'billion dollar' hacker (and was followed by at least three books and one movie of the events), helped create a context in which hackers formation as a self-recognised community was partly derived from their misrepresentation. (Shimomura, 1995; Littman, 1996; Goodell, 1996) In this context, hackers began to draw on and interact with others who were thinking through the meaning of cyberspace and its politics, for example in the interactions between those forming the civil rights group the Electronic Frontier Foundation and hackers. (Sterling 1992, Brooks and Boal 1995, Thomas 2003, Jordan 2013)

If this period was largely dominated by hacking as breaking into and exploring networked computer systems this does not mean such practices were the only hacking activity. In particular, the continued rise of programming as a profession lead to increasing numbers of programmers working within an expertise based proletariat, while at the same time Free Software continued to spread as an idea and a number of key projects began that would contribute ways of conducting large-scale programming efforts within Free Software principles and would contribute significant programmes such as Emacs (text editor for programming), Apache (web server) and Linux (operating system). As Kelty noted, Free Software emerged in the 1990s as something that could be called a movement

and which would provide key principles by which ongoing conceptions of the meaning of cyberspace and its politics would change. (Kelty, 2008; Williams, 2004) Within this movement hacking meant something other than cracking, often referring to a clever or impressive feat of programming, and usually associated with particular cultures of programming such as the Unix philosophy. Here hackers took a particular state of a programme, situated themselves within it and then altered its potential actions by reprogramming or extending the capabilities of the programme with new code. At the same time that hacking was becoming widely associated with cracking, hackers themselves questioned this, leading to the at times seemingly interminable cracking versus hacking debate. Free software communities were key in creating different, significant practices within information technocultures. From this strand would begin to grow further changes in the conception of hackers, pulling it away from cracking and locating it squarely within the innovative political practices of Free Software that included openness, property as distribution, and loose, networked production forms. (Kelty, 2008; Coleman, 2012; Weber, 2004)

I mentioned toward the end of the previous phase of hacking's history the emergence of a theme across practices of both changing and relying on a technology. Cracking is an exemplar of this in the way its core practice involves knowing a particular information technology and its characteristics, particularly its faults, in order to use those characteristics to re-purpose that technology, altering legal, social and cultural factors in the process. Each crack will interrogate the logics of particular expressions (embodied or materialised in particular instances) of information techno-cultures, by having to rely on their logics—that are cultural as well as technical, as social engineering (or tricking someone into giving out a password) dramatises—and then changing those logics. Here we see emerging the way hacking's practices express, or enunciate, the rationality of information techno-cultures by exemplifying its logics both technical and discursive.

If the golden age of hacking was really the golden age of hacking-as-cracking then it changed when hacking began to shift on a number of fronts. The criminalisation of cracking proceeded in many countries, putting hackers-as-crackers on a different relationship with security authorities, and with prosecution increasingly likely, awareness of which grew in the hacking communities (sometimes humorously such as the 'spot the Federal agent' competition at annual hacker conference Defcon). (Wellen, 2009) Threaded through this period is the ongoing articulation of gender as a form of misogyny which created cultures and practices that defined women as ‘different’ to hackers and excluded them from cracking practices. (Jordan and Taylor 1998) At the same time, it was increasingly clear that use of the internet was growing rapidly, particularly with the rise of the World Wide Web during this period. Capitalists were beginning to pay attention and the first internet gold rush, the dot.com boom and bust of the early twenty-first century, was looming. Hacking was beginning to shift in this context in which more and more people were coming to the place called cyberspace, a name that would recede as the internet became increasingly integrated into people's lives rather than being something people ‘went to’.

Hacking Divisions: A History of Hacking Part III

Media, police and computer security industry pressures explain some of the changes that brought the end of hacking's identification with cracking, but there was also the return of other elements of hacking. These, like free software advocacy, had largely always been there but were either ignored in the publicity around cracking or were minor, if not arcane, pursuits. Hacking as a set of practices that underpin a community begins to divide and four of these divisions require attention as the twenty-first century arrived: rise of cybercrime; emergence of hacktivism; new prominence of free software and emergence of open source; and, the idea that hacking is an ethic of creativity.

The case that cybercrime provoked for many years an irrational and extreme response in relation to its actual effects was well made by Wall as the golden age moved into the series of divisions that followed it. (Wall, 2007) What a number of journalists have since traced is the way the rise of online gambling began to connect organised crime to online criminal gangs, bringing together an unholy mix of viruses, online scams, darkweb drug selling and existing organised crime expertise. (Menn, 2012: Glenny, 2012: Poulsen, 2011) Tactics like botnets (networks of hijacked computers at one person's control) trying to hold websites to ransom, increasingly sophisticated ransomeware (infecting and locking up a computer remotely until a ransom is paid) and more all began to make cybercrime if not quite the demon it had been thought to be at least turning it into something closer to it. The battle between police agencies and online crime now seems a settled and ongoing part of both online and offline life. As always care must be taken because of the history of scare stories and inflated statistics, all too often coming from companies that sell the remedy for the problem they claim to have found. But from the 2000s cybercrime was no longer mainly a scare story. (Wall, 2008; Menn, 2012; Glenny, 2012; Poulsen, 2011)

A second shift from the 'golden age' is the rise of politically motivated hacking, usually called hacktivism. This is different to the use of the internet for publicity or communication by activist groups, something that occurred almost immediately such communication became available, but refers to the conception of the internet as a place capable of specific and different political actions. Paul Taylor and I conceptualised early hacktivism as having two streams. One was mass action hacktivism which attempted to reinvent mass demonstration and civil disobedience tactics in online settings. Second was internet infrastructure hacktivists who built tools to try and embed free and secure access to providing and receiving information over the internet. The latter connected strongly to the re-rise of free software and coding as core elements of hacking. In more recent times, a further wave of hacktivists have used cracking techniques to obtain information to leak, have used

denial of service attacks and have continued building infrastructure to support popular political activism. Coleman's ethnography of Anonymous both demonstrates the extension of hacktivism and its continued use of both mass online actions and the defence of digital infrastructure. (Coleman, 2014; Jordan, 2015; Jordan and Taylor, 2004; Sauter, 2014)

The work of the Free Software Foundation in creating software tools widely used by programmers, such as Gnu Emacs or the Gnu Complier Collection (GCC), and of articulating why doing this with distributive licences that allow common access to source code is a political imperative combined to underpin a rising interest in free software. The rise of widely used and, for many, superior forms of software like Apache and Linux further intensified interest here. Turning the Netscape web browser into a version of free software, eventually leading to the Firefox browser, drew attention to free software and its core principles of clever programming and access to source code as elements of hacking. (Weber, 2004; Williams, 2004) In the context of the dot.com bust, free software and its novel methods were perceived by some as a means to reinvigorate internet industries but the 'free' was also deemed by some to be unfriendly to business. Open Source was then invented as a business friendly version of free software programming techniques and ideas about property, leading to the integration of hacker principles embedded in free software into forms of capitalist profit making. With the rise of businesses (like Google) powered by free software, particularly Linux, hacking began to be seen by some not as the province of crackers, criminals or political activists but as a core principle of a new economy. (O'Reilly, 2005; Raymond, 2001; DiBona et.al., 1999)

The latter idea was extended by some into the celebration of hacking as a new principle of a new society. The journal *Wired* championed many ideas here, building on prior writing such as that in magazine *Mondo 2000*. (Rucker et.al., 1992) The work of Kevin Kelly became influential, even if it

also embodied a particularly libertarian interpretation. (Kelly, 2011, 1994; Wolff, 1999) Himanen's rather thin case for hacking as the ethic of a new kind of work, received significant attention. demonstrating he had touched on something that, like Kelly, was being thought about widely. (Himanen, 2001; Jordan, 2008, pp. 6-8) Wark's more left-wing take on hacking as a revolutionary ethos drew on similar ideas but at least cast them more solidly on a philosophical foundation. (Wark, 2004) All these efforts drew widespread attention, while also diluting hacking's previous connection to computers and information networks, suggesting that hacking was an ethic that could be applied to anything. In this work we find an endpoint of hacking because when considered purely as an ethic concerned with such vague ideas as 'cleverness', hacking dissolves from any particular kind of social practice into vague ahistorical claims.

These four phenomena significantly altered hacking. They created and drew from a process by which hacking was pulling away from the connotation of illicit cracking of computer networks, even as such cracking continued, and returned in particular broadened the idea of hacking as clever uses of information technology. Changes came with a dark side in cybercrime and wider social responsibility in hacktivism's connections to global resistance and human rights movements. All these practices rely on the interrogation of techno-cultures to change them while relying on them, and this is a process that uncovers and articulates its rationalities. This interrogation of such rationalities is something that is carried forward into these changes within hacking. Cybercrime repeats this, for example in phishing in which criminals seek out the best way to mimic a site to entrap someone which uncover the logics of trust online or in Free Software whose central commitment to being able to access the code in order to change it articulates clearly hackers' practices. As all these new ways of expressing the rationality of information techno-cultures became established, the internet was simultaneously rising to widespread mass use. The first successful and natively internet businesses were arising and the first social media networks. These trends fed

directly into the early twenty-first century.

Hacking Triumphant and Hacking Lost: A History of Hacking Part IV

From one point of view hacking can be considered triumphant in 2015, as I write. It is widely drawn on by corporations and governments, even state security agencies seek out hackers by running hack challenges to try and identify talent. At the same time, hacking remains a byword for illicit or illegal intrusions into other people's property, if anything it is more widely reviled and condemned than ever with widespread criminal activity constantly in the news and state based hacking revealed by Edward Snowden's revelations. In these times, two trends appeared that continue from previous phases with, first, a new consciousness of state based hacking and an extension of it into sabotage and, second, a new popularity for hardware hacking particularly with the rise of 3d printers and of hackspaces and fablabs. These two trends seem relatively consonant with previous hacking themes but as this account comes close to present times the view become hazier suggesting two further trends. First, as noted earlier hacking seems to have dissolved in meaning, as it comes to cover everything from the way companies design offices to the simplest of phone hacks. Second, closer to 'now' is simply harder to read.

The first trend is around nation-state based hacking. This is, to an extent, a matter of evidence catching up with actions that governments have generally kept secret or disavowed but both in terms of states' actions against each other and their concerns to manage their populations a number of typical actions have emerged that lead the state to increasingly recruit hackers and appropriate hacker practices. States acting against each other have clearly been involved in both cybersabotage and cyberespionage. For the former, the most important case is the Stuxnet worm that infiltrated Iranian state computer networks eventually leading to control of centrifuges that enriched uranium

being taken over by the software worm, that was then able to cause damage to them. (Zetter, 2014; Rid, 2013). Cyberespionage of governments against other governments, stealing state and industry secrets, has also been revealed in wide ranging programmes such as that China seems to have run against India and that the USA runs seemingly against most governments. (Deibert et.al., 2011; Deibert, 2013; Harding, 2014; Rid, 2013). At the same time a wide range of programmes governments run to manage and generate information about their own citizens have been revealed, from China's failed attempt with tracking software called Green Dam Youth Escort to the interception of data by UK and USA secret services from within such corporations as Google, Yahoo and Facebook. Here there has been a particular emphasis in the West on this expansion based on securitisation following the declaration of the 'War on Terror'. (MacKinnon, 2012; Harding, 2015; Jordan, 2015; Bamford, 2008) These programmes lead to an invasive collection of personal information that states then use profiling techniques on to try and identify whoever they are trying to catch. (Jordan, 2015; Greenwald, 2014) This use of information technologies requires expertise to run and has led to the state employing hacker cultures, much as corporations will do, to attract creative labour. This can most clearly be seen in the use by several governments of 'hack challenges' in which programmers are offered a competition to solve a particular computing puzzle, perhaps breaking into a computer, in the attempt to attract the best expertise.

The second 'continuation' trend is like Free Software in that it never went away and was present almost at the beginning of hacking and computer networks but was for a long time obscured and has only since the 2010s achieved a different popularity and public presence; hardware hacking, broadly conceived. In particular there has been a rise of permanent and semi-permanent spaces in which hacking occurs and that strongly encourage a crossover between hacking based on manipulating software to hacking based on manipulating material. The rise of FabLabs and Hackspaces are the most obvious phenomenon here, with their wide and relatively quick spread and their part in the

creation of a new sense of 'making' as an activity. (Gauntlet, 2011) There is also the rise of 3-d printers creating a whole new potential area of hacking and interesting uses of information technology expertise. (Ratto and Ree, 2012) A further example is the rapid takeup of the Raspberry Pi (two million sold in just over 18 months of its launch (Upton, 2013)), a stripped down and very cheap piece of hardware whose main use is to encourage people to understand information technology by manipulating the device. Being hands on and making changes to hardware is a longstanding tradition in hacking, but one that now seems to be spreading well beyond small communities and becoming the 'maker movement'. (Hatch, 2014; Jordan, 2008, pp. 121-3)

There were also two trends that seem rather different to those that, like state based hacking or the maker movement, extend existing hacker practices into new areas. These different trends suggest an issue about understanding the meaning of hacking by 2016. The first of these is the use of the term hacking for what seems like almost anything. This was a process first noticed when business based analysts like O'Reilly and academic analysts like Himanen and Wark designated hacking more of a practice that is widely applicable rather than something closely associated with information technologies and/or computer networks. Such an abstract use of the word hack can now be found in sites devoted to all manner of subjects such as biology hacking, curiosity hacking, health hacking and even the Ikea hackers who the Swedish furniture company tried at one point to stop. (Mulin, 2014) Here the widespread use of the term 'hack' dissipates its meaning, leading to it seeming to refer to something like a change but with its content becoming unclear. This is exacerbated by some largescale controversies that use the word hack even though the actions taken seem to have little to do with clever uses of information technologies. In particular, in the UK there was the 'phone hacking' scandal in which newspapers were found to be illicitly accessing the phone messages of a wide range of people, from a missing schoolgirl (subsequently found to have been murdered) to celebrities and politicians. (Davies, 2014) Here the action called hacking often consisted of little

more than ringing up telephone answer-machines and testing if the default password had been changed or not. While all these extensions of the word hacking seem to bear some relation to meanings already discussed, such as the illicit or the clever use of a technology, they also stretch those meanings in such a way that it is hard to locate a set of practices related to a community that constitutes hacking and this makes hacking an abstraction rendering it ghostly.

The second theme intersects with this concern because this sense in which the word 'hack' has begun to dissolve in meaning is also driven by coming ever closer to the present. For example, recently attending an opening event at a FabLab it was noticeable in this case that there was a very strong arts component in the conception of this particular lab. Artists tend to be present in many FabLabs and their presence was not the interesting fact, but their relative importance in framing the understanding of what innovation is and what those creating the lab hoped to see it achieve were different to other FabLabs, where for example the arts are likely to be present but hardware hacking might be a main focus. Is the new FabLab I was at a harbinger of greater arts involvement in FabLabs generally or is it more a reflection of local conditions? It is impossible to say until more evidence emerges, even if we can be confident that maker labs of all kinds are likely to be influenced by both artistic and hacker practices.

These reflections on the observations I can make bring my partial and evidence-based view of what hacking means to an end. Again this section has found across hacking the intersection of changing and relying on the same information techno-cultures in ways that ensure hacking, even within states or when using the soldering iron, interrogates the rationality of information techno-cultures.

Conclusion: Hacking, Genealogy and the Situated Observer

The evidence I have presented is focused on key changes in hacking practices and their attendant cultures and communities. This emphasis on practices, cultures and communities in my research on hacking clearly relates to its beginnings in analysing hackers as a sociologist when hackers were widely pathologised as isolated, anti-social and disturbed young men. Hackers instead should be understood as developing a decentred and dispersed collective identity and to be only isolated physically by being at a computer but were always, at the same time, not only in communication with others over the internet but also had a strong tendency to form groups that met in real life. If they were in this sense 'social movement-like' then hackers were an information technology focused movement, not in the sense of being determined by their technologies but in the sense that their material and collective practices constantly attacked technologies and the determinations they produce in everyday situations in order to alter those determinations. (Jordan, 2008, pp. 132-40, Kelty 2008) This connection to practices and communities supports the view that if hacking is to mean anything then it cannot be extended too far such that any practice might be considered a hack or it will become a ghostly presence. The key example from the last forty years of hacking is the way hacking became during the late twentieth century reduced to cracking practices and then shifted such that by the first ten years of the twenty-first century free software practices were recognised so widely that their constructive creativity in making software was to many a model of a new social or business practice called hacking.

What my genealogical tracing shows exists across all these different phases, practices, histories, cultures and communities of hacking, is hacking's specificity as the engagement with redetermining information technologies. Redetermination assumes an already determining relationship in which information technologies make only certain actions possible but that this determination is precisely the object of practices to redetermine it. As has been argued these redeterminations are not only ‘technical’ in the sense of manipulating software and hardware abut are also expressive in the

attitudes, such as transgression and masculinity, and cultures, such as the various understandings of 'best' ways of coding or of 'clever' technical tricks. This drive to redetermination, to always being in a determinative relationship with information technologies while also always using that situation to change determinations, is a way of expressing and exploring the rationality of information technology. Hackers reveal or express in their practices the rationality of information techno-cultures by grappling constantly with their determinations and demonstrating where and how redetermination is possible and, accordingly, what the logics of information techno-cultures are even as they change and develop. Such logics are not separate to discourses, cultures and expressions but are instead understood as being always related to recurrent expressions and cultures that populate hacking as a practice.

Hacking practices through their constant determination and redetermination of information techno-cultures articulate in information techno-cultures a combination of malleability and openess to change combined with the ability to create a field in which certain actions are enabled or determined to be possible. The rationality of information techno-cultures is to be simultaneously open to change—as hackers demonstrate constantly through their appropriation and rearticulation of devices and their effects—and as creating particular persistent fields in which certain kinds of practices and actions are not only made possible but are incited to the extent that they are determined to occur in relation to each other. Moreover, the peculiarity of these as information practices is that the very field of actions, that which determines what counts as an action in a particular field and what constitutes an action, is itself open to change through these practices. Hackers constantly alter the rules of action not only in changing the actions but in what makes action possible and this is a core tenet of the rationality of information technology. This is a complex rationality in which it is possible to see at the same time almost unceasing change with new apps, new devices and new kinds of social interactions (from the 'likes' of Facebook to the

swiping of Tindr) and to see persistent sets of practices and cultural forms (textual interaction whether in email, in online games, in comments or online fora remain a key type of online communication with characteristics identified as early as the 1980s). This intersection of malleability and persistence in the creation of digital infrastructures most closely captures the nature or hacking across all the phases my genealogy proposes. At this point analysis of hacking needs to connect to software studies as it is the malleability of infrastructures that software underpins that hackers most powerfully rely on and enact; it is software determined contexts that are most fluid in redeterminations. (Fuller 2008) This rationality is also not free of politics, as the place of gender inequalities within hacking attest. (Jordan 2105) Hackers are defined by this intersection in which no matter what phase or kind of practices are looked at hackers situate themselves in relation to information techno-cultures both relying on and then altering those techno-cultures. Neither should this analysis be understood as referring only to technical matters, Free Software's alteration of the idea of property as exclusion or its new forms of organising production are legal, cultural and organisational hacks within information techno-cultures.

Genealogy helps us to locate the importance of hackers and the attention they rightfully draw because their practices explore and reveal the rationality of the core techno-culture of our time. It is in this sense that hackers express the rationality of information techno-cultures because they operate that rationality in their daily practices.

Bibliography

Bamford, J. (2008) *The Shadow Factory*, New York: Anchor

Barad, K. (2007) *Meeting the Universe Halfway: quantum physics and the entanglement of matter and meaning*, London: Duke University Press

Barnet, B. (2013) *Memory Machines: the evolution of hypertext*, London: Anthem Press

Berry, D. (ed) (2012) *Understanding Digital Humanities*, Basingstoke: Palgrave Macmillan

Bloor D. (1997) *Wittgenstein Rules and Institutions*, London: Routledge

Brook, J. and Boal, I. (eds) (1995) *Resisting the Virtual Life: The Culture and Politics of Information*, San Francisco: City Lights

Brunton, F. (2013) *Spam: A Shadow History of The Internet*, Cambridge, Mass.: MIT Press

Coleman, G. (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso

Coleman, G. (2012) *Coding Freedom: The Ethics and Aesthetics of Hacking*, Princeton: Princeton University Press

Corneliussen, H.G. (2012) *Gender-Technology Relations: Exploring Stability and Change*, Basingstoke: Palgrave Macmillan

Davies, N. (2014) *Hack Attack: how the truth caught up with Rupert Murdoch*, London: Chatto and Windus

Deibert R. (2013) *Black Code: Inside the Battle for Cyberspace*, Toronto: McClelland and Stewart

Deibert R., Palfrey J,. Rohozinski R. and Zittrain J. (eds.) (2011) *Access Contested: Security Identity and Resistance in Asian Cyberspace*, Cambridge Mass.: MIT Press

Deleuze G. (1994) *Difference and Repetition*, London: Athlone Press

DiBona C., Ockman, S. and Stone, M. (eds) (1999) *Open Sources: Voices from the Revolution*, Sebastapol CA.: O'Reilly

Foucault, M. (1997) 'On the Genealogy of Ethics', in Rabinow, P. (ed) (1997) *Michel Foucault: Ethics, Subjectivity and Truth; Essential Works of Foucault 1954-984 Volume One,* New York: The New Press, pp. 253-80

Foucault, M. (1977) 'Nietzsche, Genealogy, History', in, Bouchard, D. (ed) (1977) *Language, Counter-memory, Practice: selected essays and interview by Michel Foucault,* Ithaca, N.Y.: Cornell University Press, pp. 139-64

Fuller, M. (ed) (2008) *Software Studies; a Lexicon*, Cambridge, Mass.: MIT Press

Goodell, J. (1996) *The Cyberthief and the Samurai: The True Story of Kevin Mitnick and the Man Who Hunted Him Down*, New York: Dell

Gauntlet, D. (2011) *Making is Connecting*, Cambridge: Polity

Glenny M. (2012) *Dark Market: How Hackers Became the New Mafia,* London: Vintage Books

Goldstein, E. (2008) *The Best of 2600 [A Hacker Odyssey]*, Indianapolis; Wiley

Grenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State,* London: McLelland and Stewart

Haraway, D. (1991) *Simians, Cyborgs, and Women: the reinvention of nature*, London: Free Association Books

Hafner, K. and Markoff, J. (1991) *Cyberpunks: Outlaws and Hackers on the Computer Frontier*, London: Corgi

Harding L. (2014) *The Snowden Files: the Inside story of the World's Most Wanted Man,* London: Guardian Books

Harding, S. and Hintikka, M. (eds) (2003) *Discovering Reality: feminist perspectives on epistemology, metaphysics, methodology and philosophy of science,* Dordrecht: Kluwer

Hatch, M. (2014) *The Maker Movement Manifesto*, New York: McGraw-Hill Education

Himanen P. (2001) *The Hacker Ethic: a radical approach to the philosophy of business,* New York: Random House

Jordan, T. (2015) *Information Politics: Liberation and Exploitation in the Digital Society*, London: Pluto

Jordan, T. (2013) *Internet, Culture and Society: Communicative Practices Before and After the Internet*, London: Bloomsbury

Jordan, T. (2008) *Hacking: digital media and technological determinism,* Cambridge: Polity

Jordan, T. (1999a) *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, London: Routledge

Jordan, T. (1999b) 'New Space New Politics?: cyberpolitics and the Electronic Frontier Foundation' in Jordan T. and Lent A. (eds.) (1999) *Storming the Millennium: the new politics of change* (London: Lawrence and Wishart)

Jordan, T. and Taylor, P. (2004) *Hacktivism and Cyberwars: Rebels With a Cause?*, London: Routledge

Jordan, T. and Taylor, P. (1998) 'A Sociology of Hackers', *Sociological Review*, 46 (4), pp. 675-93

Kelly, K. (2011) *What Technology Wants*, New York: Viking

Kelly, K. (2004) *Out of Control: The New Biology of Machines*, London: Fourth Estate

Kelty C. (2008) *Two Bits: The Cultural Significance of Free Software,* Raleigh: Duke University Press

Kollock, P. and Smith, M. (eds) (1998) *Communities in Cyberspace*, London: Routledge

Landow, G. (2006) *Hypertext 3.0: critical theory and new media in the era of globalization*, Balitmore: Johns Hopkins Press

Lapsley P. (2013) *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell,* New York: Grove Press

Letherby, G. (2003) *Feminist Research in Theory and Practice*, Buckingham: Open University Press

Levy, S. (2001) *Crypto: Secrecy and Privacy in the New Code War*, London: Allen Lane

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*, London: Penguin

Littman, J. (1997) *The Watchman: The Twisted Life and Serial Crimes of Kevin Poulsen*, Boston: Little Brown

Littman, J. (1996) *The Fugitive Game: Online with Kevin Mitnick, The Inside Story of the Great Cyberchase*, Boston: Little Brown

Macey, D. (1994) *The Many Lives of Michel Foucault*, London: Pantheon

MacKinnon R. (2012) *Consent of the Networked: the worldwide struggle for internet freedom*, New York: Basic Books

Menn J. (2010) *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet*, New York: Public Affairs

Miller, D. (1994) *The Passion of Michel Foucault*, New York: Doubleday

Mitnick K. (2011) *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, New York: Little Brown and Company

Morris, M. (1979) 'The Pirate's Fiancee', in Morris, M. and Patton, P. (eds) (1979) *Michel Foucault: power, truth, strategy*, Sydney: Feral Publications, pp. 148-68

Mulin, J. (2014) 'Ikea Waits Eight Years, Then Shuts down Ikeahackers Site With Trademark Claim', *Ars Technica* website, available at http://arstechnica.com/tech-policy/2014/06/ikea-waits-8-years-then-shuts-down-ikeahackers-site-with-trademark-claim/ , accessed August 2014

O'Reilly, T. (2005) 'What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software', *O'Reilly Media Website*, available at http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, accessed January 2015

Peterson, J. (2012) *Playing at the World: A History of Simulating Wars, People and Fantastic Adventures from Chess to Role-Playing Games*, San Diego: Unreason Press

Poulsen K. (2011) *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*, New York: Random House

Quittner, J. and Slatalla, M. (1995) *Masters of Deception: The Gang that Ruled Cyberspace*, London: Vintage

Ratto, M. and Ree, R. (2012) Materializing Information: 3D printing and social change', *First Monday*, 17 (7), available at http://firstmonday.org/ojs/index.php/fm/article/view/3968/3273, accessed August 2014

Raymond, E. (2001) *The Cathedral and the Bazaar: Musing on Linux and Open Source by an Accidental Revolutionary*, Sebastapol CA.: O'Reilly

Rheingold, H. (1994) *The Virtual Community: Surfing the Internet*, London: Minerva

Rid, T. (2013) *Cyberwar Will Not Take Place*, London: Hurst

Rosenberg, S. (2008) *Dreaming in Code*, New York: Three Rivers Press

Rucker, R., Sirius, R. and Miu Q. (1992) *Mondo 2000 Users' Guide To The New Edge*, New York: HarperCollins

Sauter, M. (2014) *The Coming Swarm: DDOS Actions, Hacktivism and Civil Disobedience*, London: Bloomsbury

Shepherd, T., Harvey, A., Jordan, T., Srauy, S. and Miltner, K. (2015) 'Histories of Hating', *Social Media + Society*, 1 (2), pp.1-10

Shimomura, T. (1995) *Takedown: The Pursuit and Capture of Kevin Mitnick, the World's Most Notorious Cybercriminal By the Man Who Did It; with John Markoff*, London: Secker and Warburg

Sterling, B. (1992) *The Hacker Crackdown*, London: Viking

Taylor P. (1999) *Hackers: Crime in the Digital Sublime*, London: Routledge

Thomas, D. (2003) *Hacker Culture*, Minneapolis: University of Minnesota Press

Thomas, J. (2005) 'The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the 'Golden Age' of Hacking', *New, Media and Society*, 7 (5), pp. 599-624

Upton, K. (2013) 'Two Million', *Raspbery Pi Blog*, available at http://www.raspberrypi.org/two-million/, accessed August 2014

Wall, D. (2008) 'Cybercrime and the Culture of Fear: Social Science fiction(s) and the production of knowledge about cybercrime', *Information, Communications and Society* 11 (6), pp. 861-884

Wall, D. (2007) *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity

Wark, M. (2004) *A Hacker Manifesto,* Cambridge Mass.: Harvard University Press

Weber S. (2004) *The Success of Open Source,* Cambridge Mass.: Harvard University Press

Wellen, A. (1999) 'Def Con's Sport: Spot the Fed', *ZDNet*, available at http://www.zdnet.com/article/def-cons-sport-spot-the-fed/, accessed January 2015

Wolff, M. (1999) *Burn Rate: How I Survived the Gold Rush Years on the Internet*, New York: Touchstone

Williams, S. (2012) *Free As In Freedom: Richard Stallman's Crusade for Free Software*, Sebastapol: Oreilly

Zetter, K (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New York: Crown Publishers

1 The irony should be acknowledged here of the debate over Foucault's relation to feminism, which can perhaps best be shortened to Morris' poetic point made after looking at androcentrism in Foucault's writing that 'any feminists drawn in to sending Love Letters to Foucault would be in no danger of reciprocation' (Morris 1979; 152)